

**IN THE UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF OHIO
EASTERN DIVISION**

In the Matter of the Search of:) **Case No:** 2:24-mj-37
)
The content of associated files of Cybertipline report)
165524186 and Cybertipline report 166336474,)
which are located at the National Center for Missing)
and Exploited Children (NCMEC), and were)
provided to NCMEC by Microsoft) **UNDER SEAL**

**AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR A SEARCH WARRANT**

I, John Bartolucci (Your Affiant), a Task Force Officer with Homeland Security Investigations (HSI) being duly sworn, hereby depose and state:

I. EDUCATION TRAINING AND EXPERIENCE

- 1) I have been a sworn law enforcement officer for over 18 years with extensive training and experience. I am currently employed with the Ohio Internet Crimes Against Children Task Force assigned as a sworn Deputy Sheriff Detective with the Franklin County Sheriff's Office and Homeland Security Investigations as a Task Force Officer. I am a graduate of the Federal Bureau of Investigation's Cyber Investigations Certification Program as well as a myriad of extensive training from the United State Secret Service's National Computer Forensic Institute.
- 2) While performing my duties as a Deputy Sheriff Detective with FCSO and Task Force Officer with HSI, I have participated in various investigations involving computer-related offenses and have executed search warrants, including those involving searches and seizures of computers, digital media, software, and electronically stored information. As part of my duties, I investigate various criminal child exploitation offenses, including those in violation of 18 U.S.C. §2252, and 2252A.
- 3) As a TFO with the HSI, I am authorized to investigate violations of the laws of the United States and to execute warrants issued under the authority of the United States.

II. PURPOSE OF THE AFFIDAVIT

- 4) This affidavit is submitted in support of an application for a search warrant for the files submitted in connection with CyberTipline Report 165524186 and 166336474 (more fully described in **Attachment A** and referred to collectively as the **CyberTipline Reports**), and the data located therein that were forwarded to the National Center for Missing and Exploited Children (NCMEC) by Microsoft. There is probable cause to believe that the items in the **CyberTipline Reports** in **Attachment A** are items described in **Attachment B**, being evidence, fruits, and instrumentalities of violations of 18 U.S.C. §§ 2252 and 2252A – the distribution/receipt/possession of visual depictions of minors engaged in sexually explicit conduct (hereinafter “child pornography”).
- 5) The facts and statements set forth in this affidavit are based on my knowledge, experience, and investigation, as well as the knowledge, experience, and investigative findings of others with whom I have had communications about this investigation, including other law enforcement officers and agents. Since this affidavit is being submitted for the limited purpose of securing a search warrant, I have not included each and every fact known to me concerning this investigation. I have set forth only the facts I believe are necessary to establish probable cause that items as outlined in **Attachment B** are located within the **CyberTipline Reports**. I have not omitted any facts that would negate probable cause.
- 6) The court has jurisdiction to issue the proposed warrant because it is a “court of competent jurisdiction” as defined in 18 U.S.C. § 2711. Specifically, the Court is a district court of the United States that has jurisdiction over the offense being investigated, see 18 U.S.C. § 2711(3)(A)(i).

III. APPLICABLE STATUTES AND DEFINITIONS

- 7) Title 18, United States Code, Section 2252, makes it a federal crime for any person to knowingly transport, receive, distribute, possess or access with intent to view any visual depiction of a minor engaging in sexually explicit conduct, if such receipt, distribution or possession utilized a means or facility of interstate commerce, or if such visual depiction has been mailed, shipped or transported in or affecting interstate or foreign commerce. This section also prohibits the reproduction for distribution of any visual depiction of a minor

engaging in sexually explicit conduct, if such reproduction utilizes any means or facility of interstate or foreign commerce or is in or affecting interstate commerce.

- 8) Title 18, United States Code, Section 2252A, makes it a federal crime for any person to knowingly receive or distribute any child pornography using any means or facility of interstate commerce, or any child pornography that has been mailed, or any child pornography that has shipped or transported in or affecting interstate or foreign commerce by any means, including by computer. This section also makes it a federal crime to possess or access with intent to view any material that contains an image of child pornography that has been mailed, shipped or transported using any means or facility of interstate or foreign commerce, or in or affecting interstate commerce by any means, including by computer.
- 9) As it is used in 18 U.S.C. §§ 2252, the term “sexually explicit conduct” is defined in 18 U.S.C. § 2256(2)(A) as actual or simulated: sexual intercourse, including genital-genital, oral-genital, anal-genital, or oral-anal, whether between persons of the same or opposite sex; bestiality; masturbation; sadistic or masochistic abuse; or lascivious exhibition of the genitals or pubic area of any person.
- 10) As it is used in 18 U.S.C. § 2252A(a)(2), the term “child pornography”¹ is defined in 18 U.S.C. § 2256(8) as: any visual depiction, including any photograph, film, video, picture, or computer or computer-generated image or picture, whether made or produced by electronic, mechanical, or other means, of sexually explicit conduct, where: (A) the production of such visual depiction involves the use of a minor engaging in sexually explicit conduct; (B) such visual depiction is a digital image, computer image, or computer generated image that is, or is indistinguishable from, that of a minor engaging in sexually explicit conduct; or (C) such visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaging in sexually explicit conduct.
- 11) The term “sexually explicit conduct” has the same meaning in § 2252A as in § 2252, except that for the definition of child pornography contained in § 2256(8)(B), “sexually explicit conduct” also has the meaning contained in § 2256(2)(B): (a) graphic sexual intercourse, including genital-genital, oral-genital, anal-genital, or oral-anal, whether

¹ The term child pornography is used throughout this affidavit. All references to this term in this affidavit and all Attachments hereto include both visual depictions of minors engaged in sexually explicit conduct as referenced in 18 U.S.C. § 2252 and child pornography as defined in 18 U.S.C. § 2256(8).

between persons of the same or opposite sex, or lascivious simulated sexual intercourse where the genitals, breast, or pubic area of any person is exhibited; (b) graphic or lascivious simulated (i) bestiality, (ii) masturbation, or (iii) sadistic or masochistic abuse; or (c) graphic or simulated lascivious exhibition of the genitals or pubic area of any person.

- 12) The term “minor”, as used herein, is defined pursuant to Title 18, U.S.C. § 2256(1) as “any person under the age of eighteen years.”
- 13) The term “graphic,” as used in the definition of sexually explicit conduct contained in 18 U.S.C. § 2256(2)(B), is defined pursuant to 18 U.S.C. § 2256(10) to mean “that a viewer can observe any part of the genitals or pubic area of any depicted person or animal during any part of the time that the sexually explicit conduct is being depicted.”
- 14) The term “visual depiction,” as used herein, is defined pursuant to Title 18 U.S.C. § 2256(5) to “include undeveloped film and videotape, and data stored on computer disk or by electronic means which is capable of conversion into a visual image.”

VII. CYBERTIPLINE REPORTS

- 15) The National Center for Missing and Exploited Children (“NCMEC”) is an organization that, among other things, tracks missing and exploited children and serves as a repository for information about child pornography. Federal law requires NCMEC to operate the CyberTipline and requires Electronic Service Providers to report apparent instances of child pornography offenses. Providers also have the discretion to submit reports concerning planned or imminent child pornography offenses. Companies that suspect child pornography has been stored or transmitted on their systems report that information to NCMEC in a CyberTipline Report (or “CyberTip”). The Electronic Service Provider submits the report and uploads content to NCMEC via a secure connection. Aside from required information such as incident type, date, and time, reporters can also fill in voluntary reporting fields such as user or account information, IP addresses, or information regarding the uploaded content itself, as well as other information it may have collected in connection with the suspected criminal activity. The Electronic Service Provider may or may not independently view the content of the file(s) it uploads. Using publicly available search tools, NCMEC then attempts to locate where the activity occurred based on the information the Electronic Service

Provider submits, such as IP addresses. NCMEC then packages the information from the Electronic Service Provider along with any additional information it has, such as previous related CyberTips, and sends it to law enforcement in the jurisdiction where the activity is believed to have occurred.

VIII. INVESTIGATION AND PROBABLE CAUSE

- 16) On or about August 2, 2023, the Franklin County Internet Crimes Against Children (ICAC) task force received a CyberTipLine report from the National Center for Missing and Exploited Children (NCMEC). The CyberTipLine report, which was dated May 29, 2023, indicated that two images of child sexual abuse material had been uploaded to a BingImage search engine². The first image uploaded to BingImage depicted a nude prepubescent female with her vagina exposed to the camera and the second image depicted a collage made up of twelve photographs. Contained within the collage of photographs were images of prepubescent female minors engaged in acts of masturbation, bestiality, bondage, and sex acts with adults including oral and vaginal sex, as well as the lascivious display of their vaginas and anuses.
- 17) When the NCMEC report was received by the ICAC, subscriber information had already been obtained for the IP address utilized for the upload which resolved to Charter Communications. Subscriber information from Charter Communications came back to Steve Chinn (**CHINN**) at an address of 935 Quay Avenue, Apartment H, in Columbus, Ohio.

² This search engine allows individuals to take an image from their own device, drag/drop the images into a search box via Bing, and then upload image into BingImage search in an effort to search Bing for image files similar to those that were uploaded.

- 18) The information provided by Charter Communications also revealed that **CHINN**'s subscriber telephone number and email address were (614) 946-1075 and manychinns@gmail.com, respectively.
- 19) After receiving the NCMEC referrals, the Franklin County ICAC gathered information on **CHINN** and learned that the Quay Avenue apartment was owned by **CHINN**. **CHINN** also had his vehicle, a brown 2014 Honda Civic, registered at that address and subsequent surveillance by law enforcement identified **CHINN**'s vehicle at the apartment as well.
- 20) On August 4, 2023, law enforcement further confirmed that WiFi connections and available networks near the Quay Avenue apartment were all secured which indicated that for an individual to utilize the IP address identified in the NCMEC report, the user would have to have the password to gain access. Further investigation also revealed that at the time the BingImage upload was made, **CHINN** was employed as a Franklin County Public Defender.
- 21) On or about August 16, 2023 at approximately 6:15am, Grandview Heights Police along with the Franklin County ICAC executed a residential search warrant at **CHINN**'s residence on Quay Avenue. **CHINN** was present on scene and declined to speak with law enforcement. A black LG cell phone was seized off **CHINN**'s person. A black unbranded desktop personal computer was also located within the residence inside **CHINN**'s bedroom.
- 22) An on-scene preview of the desktop computer located in **CHINN**'s bedroom revealed images of child sexual abuse material and numerous encrypted files. The images previewed on scene all depicted prepubescent females engaged in the lascivious exhibition of their genitalia, masturbation, and sex acts with adults.
- 23) **CHINN** was placed under arrest and initially charged in Franklin County for Pandering Sexually Oriented Matter Involving a Minor and Pandering Obscenity.

24) Forensic review of the seized devices by your affiant revealed child sexual abuse material on the desktop computer belonging to **CHINN**. In total, approximately 4,286 images of child sexual abuse material were identified in both the carved and parsed locations within the computer. No metadata was available for the carved images, which were located in the cache portions of the device, further indicating that the file had been previously deleted by **CHINN**. The recovered images contained within the parsed locations had a last access date listed as August 2023 for all recovered child sexual abuse material that **CHINN** downloaded.

25) One of the images, titled *Artifact # 589505*, depicted a prepubescent female with her hands bound, blindfolded, and kneeling while an adult male holds a whip to her neck with one hand and in the other, holds his penis in her mouth. Another image, titled *Artifact # 590749*, depicted a prepubescent toddler with an adult male penis inserted into her anus at the same time an adult male hand spreads apart her vagina.

26) The desktop computer also contained 19 videos depicting prepubescent minors engaged in sexually explicit conduct, again with the last access date of August 2023. All of the child pornography images and videos recovered from **CHINN**'s desktop computer depicted babies, toddlers, and prepubescent minors engaged in the lascivious display of their genitalia, masturbation, sex acts with adults and other minor children, bestiality and/or bondage.

27) In reviewing other artifacts on the desktop computer of **CHINN**, forensic analysts noted that the computer was secured with a Microsoft account and a password and the saved login credentials were under the username `mannychinns@gmail.com`. In addition, on or about August 10, 2023, Chrome Login artifact data indicated that the username `"smchinn@franklincountyohio.gov"` was used to login to `https://login.microsoft.com`. Furthermore, carved social media artifacts were recovered which indicated that on or about

August 11, 2023 at 10:10pm, the website <https://vk.com> was accessed. Vk.com is also referred to as Vkontakte and is a Russian social media site known to be utilized for the download and exchange of child sexual abuse material. Law enforcement noted that **CHINN** intentionally deleted or attempted to remove evidence of this activity based on the fact that this information was recovered from the carved portion of the desktop computer. Of note is that all but three of the child pornography images/videos recovered from the parsed space had a creation date/time of on or about August 11, 2023 at 10:10pm through on or about August 12, 2023 at 10:02am and were recovered in the "...Horizon\Downloads" directory indicating that **CHINN** was downloading the files off the internet, from the vk.com website specifically, on those respective dates and times.

- 28) **CHINN** was indicted by a federal grand jury for charges related to the above facts on September 19, 2023 and his case is currently pending before Judge Sarah D, Morrison under case number 2:23-cr-188.
- 29) After **CHINN** was indicted, law enforcement learned that two additional CyberTipLine reports were generated, also related to **CHINN**. More specifically, your affiant learned that on or about July 1, 2023, and on or about July 14, 2023, Microsoft submitted two CyberTipline Reports, specifically report 165524186 and 166336474, to the NCMEC. As reported by Microsoft, and specifically BingImage again, the primary incident type was listed as "Child Pornography" (possession, manufacture, and distribution) and the incident times were listed as July 1, 2023, 05:54:39 UTC, and July 14, 2023, 05:35:26 UTC respectively.
- 30) BingImage also uploaded file(s) in connection with the report. Two files were uploaded under CyberTipline Report 165524186, one of which was reviewed by both Microsoft and NCMEC. An additional file was uploaded under CyberTipline Report 166336474, which was reviewed by Microsoft and NCMEC as well.
- 31) The following additional information for CyberTipline Report 165524186 was provide by Microsoft as well:
 - BingImage

- Telephone Number: 614-946-1075
- IP Address: 2603:6010:4900:1b4:298c:ba99:8cc2:d704 at 07-01-2023 05:54:39 UTC
- User Provided account Full Name: Stephen Chinn
- File 1 Name: 97170dd6-483d-45cb-8702-8bd6c73e2ca5.jpg

32) The ESP reported the following additional information for CyberTipline Report 166336474:

- BingImage
- Telephone Number: 614-946-1075
- IP Address: 2603:6010:4900:1b4:d471:e921:bcdd:56e4 at 07-14-2023 05:35:26 UTC
- User Provided account Full Name: Stephen Chinn
- File 1 Name: 9d555c04-b1d5-4056-82c2-978f0e506dc9.jpg

33) Based on my training and experience, I know that based on the additional information Microsoft gave, the uploaded content by the **CHINN** most likely contains additional evidence of his child exploitation activities and images depicting minors engaged in sexually explicit conduct as outlined by the type of content **CHINN** was searching and possessing throughout the course of the investigation into him.

34) Therefore, there is probable cause to believe that the content of the file(s) that Microsoft reported in connection with the submitted CyberTipline Reports noted above contain at least one image of previously identified child pornography. This is also based on the information above, including that your affiant has reason to believe that **CHINN** is the owner of the BingImage accounts, and the uploads likely contain images which may constitute contraband and evidence of criminal violations of 18 U.S.C. §§ 2252 and 2252A – the distribution/receipt/possession of visual depictions of minors engaged in sexually explicit conduct.

XI. CONCLUSION

35) Based on the investigation described above, probable cause exists to believe that inside the files that Microsoft uploaded in connection with the above CyberTipline Report (described in Attachment A), will be found evidence, fruits, and instrumentalities of a violations 18 U.S.C. §§ 2252 and 2252A – the distribution/receipt/possession of visual depictions of minors (described in Attachment B).

36) Therefore, your affiant respectfully requests that the Court issue a search warrant authorizing the search of the locations identified in Attachment A for the items listed in Attachment B.

Respectfully submitted,

NSI TFO JLB

John Bartolucci
Task Force Officer
Homeland Security Investigations

Subscribed and sworn to before me on January 24, 2024

Chelsey M. Vascara

Chelsey M. Vascara
United States Magistrate Judge
United States District Court

ATTACHMENT A
PROPERTY TO BE SEARCHED

Contents of files uploaded in connection with Cybeline Reports 165524186 and 166336474 that are currently held by the National Center for Missing and Exploited Children (NCMEC).

ATTACHMENT B
PROPERTY TO BE SEIZED

For the File(s) listed and described in Attachment A, the following items, that constitute evidence of the commission of, contraband, the fruits of crime, or instrumentalities of violations of 18 U.S.C. §§ 2252 and 2252A – the distribution/receipt/possession of visual depictions of minors engaged in sexually explicit conduct.

1. Images or visual depictions of child pornography.
2. Any and all information, notes, documents, records, or correspondence, in any format or medium, pertaining to child pornography or sexual activity with or sexual interest in minors.
3. Any and all information, documents, records, photos, videos, or correspondence, in any format or medium, pertaining to use or ownership of the File(s), or that aid in the identification of persons involved in violations of 18 U.S.C. §§ 2252 and 2252A – the distribution/receipt/possession of visual depictions of minors engaged in sexually explicit conduct